UNREDACTED VERSION OF PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

DOCUMENT SOUGHT TO BE SEALED

BOIES SCHILLER FLEXNER LLP
David Boies (admitted pro hac vice)
333 Main Street
Armonk, NY 10504
Tel.: (914) 749-8200
dboies@bsfllp.com

Mark C. Mao, CA Bar No. 236165
Beko Reblitz-Richardson, CA Bar No. 238027
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
mmao@bsfllp.com
brichardson@bsfllp.com

James Lee (admitted pro hac vice)
Rossana Baeza (admitted pro hac vice)
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
jlee@bsfllp.com
rbaeza@bsfllp.com

Alison L. Anderson, CA Bar No. 275334
M. Logan Wright, CA Bar No. 349004
725 S Figueroa St., 31st Floor
Los Angeles, CA 90017
Tel.: (213) 995-5720
alanderson@bsfllp.com
mwright@bsfllp.com

SUSMAN GODFREY L.L.P.
Bill Carmody (admitted pro hac vice)
Shawn J. Rabin (admitted pro hac vice)
Steven M. Shepard (admitted pro hac vice)
Alexander Frawley (admitted pro hac vice)
Ryan Sila (admitted pro hac vice)
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel.: (212) 336-8330
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com
afrawley@susmangodfrey.com
rsila@susmangodfrey.com

Amanda K. Bonn, CA Bar No. 270891
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Tel.: (310) 789-3100
abonn@susmangodfrey.com

MORGAN & MORGAN
John A. Yanchunis (admitted pro hac vice)
Ryan J. McGee (admitted pro hac vice)
Michael F. Ram, CA Bar No. 104805
201 N Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
rmcgee@forthepeople.com
mram@forthepeople.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ANIBAL RODRIGUEZ, SAL CATALDO, JULIAN SANTIAGO, and SUSAN LYNN HARVEY individually and on behalf of all other similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No.: 3:20-cv-04688-RS

PLAINTIFFS' NOTICE OF MOTION AND MOTION FOR CLASS CERTIFICATION AND APPOINTMENT OF CLASS REPRESENTATIVES AND CLASS COUNSEL

Judge: Hon. Richard Seeborg
Courtroom 3 – 17th Floor
Date: October 5, 2023
Time: 1:30 p.m.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Rules

PLEASE TAKE NOTICE that on October 5, 2023, at 1:30 p.m., the undersigned will appear before the Honorable Richard Seeborg of the United States District Court for the Northern District of California to move the Court, under Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3) for an order certifying two classes:

- Class 1: All individuals who, during the period beginning July 1, 2016 and continuing through the present (the "Class Period"), (a) had their "Web & App Activity" and/or "supplemental Web & App Activity" setting turned off and (b) whose activity on a non-Google-branded mobile app was still transmitted to Google, from (c) a mobile device running the Android operating system, because of the Firebase Software Development Kit ("SDK") and/or Google Mobile Ads SDK.

- Class 2: All individuals who, during the Class Period (a) had their "Web & App Activity" and/or "supplemental Web & App Activity" setting turned off and (b) whose activity on a non-Google-branded mobile app was still transmitted to Google, from (c) a mobile device running a non-Android operating system, because of the Firebase SDK and/or Google Mobile Ads SDK.

Plaintiffs seek to certify nationwide classes for Counts I, II, and III of their Complaint (Dkt. 289). Plaintiffs further move for their appointment as class representatives and to appoint David Boies and Mark C. Mao of Boies Schiller Flexner LLP, Bill Carmody of Susman Godfrey LLP, and John A. Yanchunis of Morgan & Morgan as co-lead class counsel. This Motion is based upon this Notice of Motion and Motion, the incorporated Memorandum of Points and Authorities, and the following materials, along with other materials in the record, argument of counsel, and such other matters as the Court may consider:

1. Declaration of Mark C. Mao and accompanying exhibits;
2. Declarations of Amanda Bonn, John Yanchunis, and James Lee;
3. Declarations for each proposed class representative;
4. Declarations (including reports) of the experts retained by Plaintiffs' counsel (Jonathan Hochman, Bruce Schneier, Michael Lasinski, Mark Keegan, and Cam Azari); and
5. Plaintiffs' proposed trial plan.

ISSUE PRESENTED

Whether the Court should certify nationwide classes to pursue these claims?

RELIEF REQUESTED

Plaintiffs respectfully ask the Court to certify the proposed nationwide classes for all three claims under both Rule 23(b)(3) and Rule 23(b)(2).

I. INTRODUCTION AND BACKGROUND

As online activity increasingly migrates from computers to smartphones, Google's reach is ubiquitous and persistent: A person using just five ***non-Google*** mobile apps has a greater than ***97%*** chance of such data being saved by Google, whose SDKs are embedded in the overwhelming majority of the most popular Android and iPhone apps. Hochman Rep. ¶¶ 355–56. Yet Google knows that creating a perception of privacy with buzzwords like "*control*" and *choice* "reassure[s]" and "build[s] trust" with users, leading to "positive business outcomes" for Google. Ex. 1 at Row 17; Ex. 2 at -102. So Google uniformly offers its account holders a Web & App Activity ("WAA") button and a supplemental setting ("sWAA"; together, "(s)WAA") to "control" whether Google "saves" data about activity on non-Google apps. *Infra* at 4 (Screens 1–3). Google explained that the WAA button "must be on" and the sWAA box "must be checked" to "let Google save" "info about your browsing and other activities" on "apps" that "use Google services." Ex. 3.

In short, Google offered its account holders an "off" switch. And Google's CEO Sundar Pichai touted this switch to Congress and the American public, testifying under oath that Google (i) allows users to "clearly see what information we have—we actually show it back to them" in My Account and (ii) "give[s] clear toggles, by category, where [users] can decide whether that information is collected [and] stored." Hochman Rep. ¶ 256. ***But it wasn't true.*** Through the Firebase Software Development Kit ("SDK") and Google Mobile Ads ("GMA") SDK (which supports AdMob and Ad Manager), Google collects, saves, and uses (s)WAA-off data. Google simply conceals that fact from users by (i) turning off "personalized" ads that could tip them off to Google's continued tracking and (ii) no longer "show[ing]" the data in users' "My Account" portal. Hochman Rep. ¶¶ 252–53. Eric Miraglia, founder of Google's Privacy and Data Protection Office, is "not aware of any setting" that *actually* allows users to stop Google from saving such data. Ex. 4 at 96:21–97:6, 128:21–129:3. Indeed—there is none. Hochman Rep. ¶¶ 249–251.

Google employees called (s)WAA a *"**loser**"* and "***completely broken***," urging a fix:

- "***WAA and other controls imply we don't log the data, but obviously we do. We need to change the description*** . . . ";

- "***I don't see how this text can't need modification***. An 'on/off' toggle means the off state is the opposite of the on state. If the on state is we log your activity, the off state is we don't log your activity";
- "***I think teams should not use user data at all if WAA is off*** . . . . It's a much cleaner story and ***what I would think most users expect***." Ex. 5, at -66; Ex. 6 at -46; Ex. 7 at -10; Ex. 8 at -22; Ex. 9 at -94.

But Google refused. Why? Because "data is the gold of the 21st century," and Google's profits and market power depend on it. Ex. 10 at -401. Google's Rule 30(b)(6) witness admitted that while Google stopped collecting a limited set of sWAA-off data generated by "App Indexing," that's only because such data "doesn't add any value." Ex. 11 at 217:7–15. By contrast, the (s)WAA-off data Googles collects from the at-issue Firebase and GMA SDKs generate substantial revenue for Google. In short, for Google's own privacy signals, profits trump privacy.

Indeed, Google leverages (s)WAA data to serve ads, to improve products and services, and to track and charge its advertisers for valuable events driven by Google Ads, a process known as "conversion tracking" or "attribution." *See, e.g.*, Ex. 12; Ex. 13 at 218:17–219:14; Hochman Rep. § VII.F.1-3. Moreover, Google's "ability to capture conversion events, as well as the ability to attribute a conversion event to a prior ad event, allows Google to demonstrate the effectiveness of its advertising platforms to the advertisers, which in turn, increases advertiser spend on Google advertising platforms." *Id.* ¶ 280; *see also* Ex. 14 at 215:15–218:4 (Rule 30(b)(6) testimony on conversions). Google has privately recognized that tracking more conversions, including through the Firebase and GMA SDKs, allows it to better compete with rival ad networks. Ex. 15 at -89.

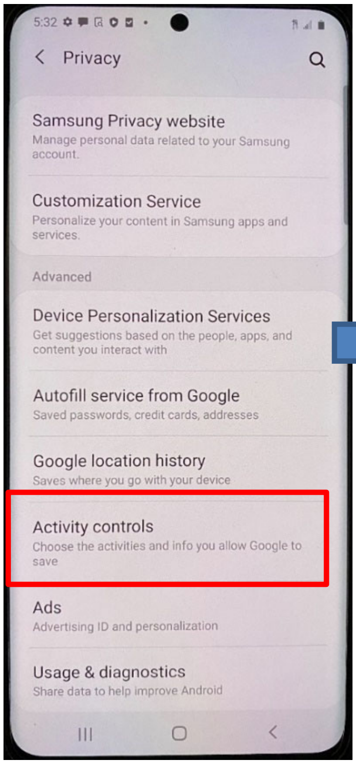
Plaintiffs seek to hold Google accountable by certifying two nationwide classes of Google accountholders who used Google's broken (s)WAA control: Class 1 for Android users and Class 2 for users of other mobile operating systems.[1] On behalf of these classes, Plaintiffs assert claims for invasion of privacy, intrusion upon seclusion, and violation of California's Comprehensive Computer Data Access and Fraud Act ("CDAFA"), all under California law, which governs these

[1] Plaintiffs' class definitions differ from the Complaint in two minor respects. *First*, Plaintiffs here use the term "Google Mobile Ads SDK" because it is the public-facing name of the product at issue. As Google employee Edward Weng testified, this term is "interchangeable" with "AdMob SDK." Ex. 16 at 59:9–12; Dkt. 289 ("FAC"), ¶¶ 4, 8, 64–66, 89 (allegations about the GMA SDK). *Second*, the class definitions refer to users who "had their [(s)WAA] setting turned off" to clarify that the classes include individuals whose (s)WAA setting was off when the Class Period began.

claims under Google's Terms of Service. Rule 23(b)(3) certification is warranted because "the ***central issues*** in the action are common to the class and can be said to predominate." *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 453 (2016) (emphasis added). In ***Google's own words***, "the ***central questions*** in the case are ***[1] what Google represented to users and [2] the actual technical functioning of the accused technology."*** Ex. 17 at 3. These "central questions," and others regarding the relief requested, will be answered with common evidence, resolving these issues "in one stroke." *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350 (2011).

<u>Central Question 1: What Google Represented</u>

How Google defined the choice offered by the (s)WAA switch is a common issue. Throughout the class period, Class 1 users were shown the following three screens on their devices, while Class 2 users could access Screens 2 and 3 through their "My Account" portal:[2]



Privacy

Samsung Privacy website
Manage personal data related to your Samsung account.

Customization Service
Personalize your content in Samsung apps and services.

Advanced

Device Personalization Services
Get suggestions based on the people, apps, and content you interact with

Autofill service from Google
Saved passwords, credit cards, addresses

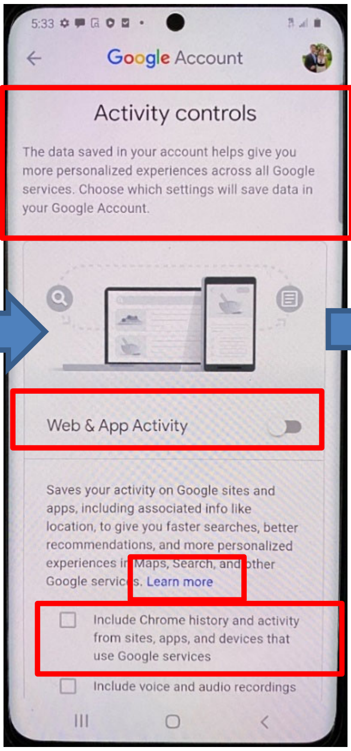
Google location history
Saves where you go with your device

Activity controls
Choose the activities and info you allow Google to save

Ads
Advertising ID and personalization

Usage & diagnostics
Share data to help improve Android

SCREEN 1



Google Account

Activity controls

The data saved in your account helps give you more personalized experiences across all Google services. Choose which settings will save data in your Google Account.

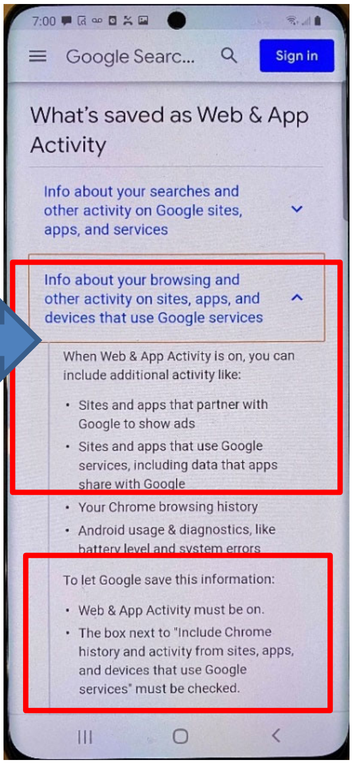
Web & App Activity

Saves your activity on Google sites and apps, including associated info like location, to give you faster searches, better recommendations, and more personalized experiences in Maps, Search, and other Google services. Learn more

□ Include Chrome history and activity from sites, apps, and devices that use Google services

□ Include voice and audio recordings

SCREEN 2



Google Searc... Sign in

What's saved as Web & App Activity

Info about your searches and other activity on Google sites, apps, and services

Info about your browsing and other activity on sites, apps, and devices that use Google services

When Web & App Activity is on, you can include additional activity like:

- Sites and apps that partner with Google to show ads
- Sites and apps that use Google services, including data that apps share with Google
- Your Chrome browsing history
- Android usage & diagnostics, like battery level and system errors

To let Google save this information:

- Web & App Activity must be on.
- The box next to "Include Chrome history and activity from sites, apps, and devices that use Google services" must be checked.

SCREEN 3

[2] *See* Ex. 18 ("Activity Controls" webpage); Ex. 3 (WAA Help Page). These disclosures were materially the same throughout the Class Period. *See* Ex. 19 at 3 (Google's counsel confirming that Screen 1 never changed); Ex. 20 at -90–91 (cataloging prior versions of "Screen 2" in effect throughout the Class Period, which are equivalent to the "Activity Controls" page of Google's website where the (s)WAA toggles are located); Ex. 21 (compilation of versions of "Screen 3," which are equivalent to the WAA Help Page on Google's website).

FAC at ¶ 90. Through these uniform disclosures, Google stated that WAA "must be on" "to let Google save" information about users' activity on "sites and apps that use Google services." And for both classes, Google's Privacy Policy reinforces this message by assuring users that "across our services, ***you can adjust your privacy settings to control what we collect and how your information is used***." Exs. 22–35 (versions of Google Privacy Policy in effect from May 2018 through today). The Privacy Policy lists these "Privacy Controls," where a "Go to Activity Controls" hyperlink brings users directly to the (s)WAA toggles. *Id*. Moreover, the Privacy Policy defines "Google services" to include "[p]roducts that are integrated into ***third-party apps*** and sites, like ***ads*** [and] ***analytics***"—i.e., the Firebase and GMA SDKs. Ex. 22 at 1; Exs. 23–35 (other versions of the Privacy Policy with same language).[3]

This Court analyzed Google's disclosures at the pleadings stage and rejected Google's argument that Plaintiffs consented to the alleged conduct. ***"[P]laintiffs did not consent to Google collecting their data, through GA for Firebase, with WAA turned 'off.'"*** Dkt. 109 ("MTD Order") at 7. Instead:

- Plaintiffs offer a ***cogent account of why they saw WAA as capable of turning off GA for Firebase's*** collection of their third-party app data. . . .
- Where, as here, a company's public-facing statements are legitimately confusing, ***it is not the public's fault for being confused. . . .***
- ***Google, through the WAA Materials, "set an expectation"*** that it would not save plaintiffs' "activity on . . . apps . . . that use Google services" unless plaintiffs turned WAA "on."

Id. at 10, 16 (citations omitted; alterations in original). As discussed above and further below, Google has produced common evidence in the form of internal emails, studies, and deposition testimony that confirm the objectively reasonable interpretation of the (s)WAA control: "off" means "off." *See supra* at 2–3 and *infra* at Section II.B.1–2.

Plaintiffs anticipate Google will argue that this case turns on individualized questions regarding each class members' privately held beliefs, rather than the objective meaning of a

[3] Earlier versions of the Privacy Policy likewise represented that "Google activity controls" allows users to "decide what types of data . . . you would like saved with your account when you use Google services." Ex. 36 at 5; Exs. 37–41 (same). And they similarly described Google's "services" to include "services offered on other sites (such as our advertising services)." Ex. 36 at 8; Exs. 37–41 (same).

proffered "off" switch. Setting aside that this argument contradicts Google's prior representations about the case's "central questions," the argument is neither legally nor factually tenable. Plaintiffs' CDAFA claim turns on whether users granted Google "permission" to collect their data. Cal. Penal Code § 502(c)(2). Any "permission" must be communicated to Google by words or conduct, after adequate disclosures describing Google's practices. But here, (s)WAA was uniformly turned *off* for all class members offered a button. Similarly, Plaintiffs' privacy tort claims turn on an objectively "reasonable" expectation of privacy, and the meaning of Google's "off" switch must be interpreted objectively. *Opperman v. Path, Inc.*, 2016 WL 3844326, at *11 (N.D. Cal. Jul. 15, 2016). This, too, can be proven with common evidence including Google's own user experience studies, one of which demonstrated in April 2020—three months before this case was filed—that "***All participants expected turning WAA toggle off to stop saving their activity***." Ex. 42 at -00, -11. Google strains to argue that "off" somehow does not mean "off."

Central Question 2: The Technical Functioning of the Accused Google Technologies

The functioning of the at-issue Google SDKs will also be proven with common evidence. Relying on classwide evidence like Google technical documentation, Plaintiffs' technical expert, Jonathan Hochman, will testify that throughout the Class Period, Google used its Firebase and Google Mobile Ads SDKs to collect, save, and use every class member's (s)WAA-off app activity data. This data is saved in so many of Google's logs and repositories that, in Google's own words, "it is not practical" to list them all. Ex. 43 at 4. (s)WAA-off data is too pervasive to catalog, even for the company whose "mission is to organize the world's information." Ex. 44.

Plaintiffs' Requested Monetary Relief

Plaintiffs will prove their monetary damages through common evidence. Plaintiffs' damages expert, Michael Lasinski, has calculated both Google's aggregate unjust enrichment (well over $500 million) and the classes' aggregate actual damages, relying on common evidence like Google's internal financial statements and revenue studies. Mr. Lasinski has also proposed methods by which any aggregate award can be apportioned among class members—methods which do not require individualized inquiries. Lasinski Rep. §§ 7–9.

Rule 23(b)(2) And Equitable Relief

Finally, the Court should also certify both classes for equitable relief under Rule 23(b)(2), as Plaintiffs "seek uniform relief from a practice applicable to all of them." *Ward v. United Airlines, Inc.*, 2021 WL 534364, at *7 (N.D. Cal. Feb. 12, 2021). Plaintiffs seek a judgment that, at a minimum, requires Google to (1) stop collecting, saving, and using (s)WAA-off app activity data, (2) delete data it already collected, (3) remove products, services, or algorithms developed or improved with that data, and (4) appoint an independent third party to verify that the injunctive relief is fully implemented. Injunctive relief is warranted to address Google's employees' unanswered cries for help.

II. ARGUMENT

A. California Law Applies to All Claims.

"Given that [Google is] headquartered in California, . . . application of California law poses no constitutional concerns in this case." *Forcellati v. Hylands, Inc.*, 2014 WL 1410264, at *2 (C.D. Cal. Apr. 9, 2014); Dkt. 305 (Google's Answer) at 4 (acknowledging its California headquarters).

There is no reason to depart from the California choice-of-law provision in the Google form contract. The classes are limited to Google accountholders, and Google has a contractual relationship with all accountholders through its Terms of Service. *E.g.*, Dkt. 139 at 21 (Google describing the Terms of Service as an "express contract"). That contract throughout the Class Period provided that "any disputes arising out of or relating to these terms or the Services" are governed by "[t]he laws of California." Exs. 45–46 at 6; *see also* Ex. 47 at 13 (choosing "California law"); Ex. 48 at 9 (same). That choice-of-law provision is especially broad because it applies to all disputes—even those "relating to" the agreement. These claims "relat[e]" to the Google Terms of Service, which "establish what [users] can expect from [Google] as you use Google services." Ex. 48 at 1. Google itself has argued that the Terms of Service "govern[] the same topic" as Plaintiffs' claims. Dkt. 139 at 20–21.

Plaintiffs do not expect Google to abandon its own choice of law, but in any event, Google cannot meet the heavy burden to do so. A California choice-of-law clause "generally will be enforced unless the other side can establish that the chosen law is contrary to a fundamental policy of the state law alternative to the contractual choice, and that the other state has a materially greater interest in the determination of the matter." *Trump v. Twitter Inc.*, 602 F. Supp. 3d 1213, 1226 (N.D. Cal. 2022). That burden is all the more crushing for Google here because Google has elsewhere embraced its form contract's California choice-of-law while (successfully) seeking dismissal of non-California claims. *See, e.g.*, *In re Nexus 6P Prods. Liab. Litig.*, 293 F. Supp. 3d 888, 934–35 (N.D. Cal. 2018). Finally, the CDAFA "expressly allow[s] an action to be brought by . . . an 'owner or lessee' [of a device] without imposing any residency requirements." *Valentine v. NebuAd, Inc.*, 804 F. Supp. 2d 1022, 1028 (N.D. Cal. 2011).

B. Plaintiffs Satisfy the Rule 23(a) Requirements.

Numerosity. Each proposed class includes many millions of users (Lasinski Rep. ¶¶ 167–69), and it would be "impracticable" to join them. Fed. R. Civ. P. 23(a)(1). Numerosity is satisfied.

Commonality. Plaintiffs' claims implicate common issues "capable of classwide resolution," and therefore satisfy Rule 23(a)(2)'s "permissive" commonality requirement. *Wal-Mart*, 564 U.S. at 350. "[E]ven a single common question will do." *Id.* at 359 (quotation marks omitted). For example, the objective meaning of Google's (s)WAA disclosures will determine on a classwide basis whether Google has "permission" to collect users' app activity data. *See infra* Section IV.B.1–2; *Utne v. Home Depot U.S.A., Inc.*, 2022 WL 1443338, at *6–7 (N.D. Cal. May 6, 2022) (Seeborg, J.) (addressing commonality and predominance together).

Typicality and Adequacy. Plaintiffs and their counsel satisfy Rule 23(a)'s typicality and adequacy requirements, which "do not pose a particularly high bar to class certification." *Ambrosio v. Cogent Commc'ns*, 2016 WL 777775, at *4 (N.D. Cal. Feb. 29, 2016) (Seeborg, J.). The claims "arise[] from the same course of events, and each class member makes similar arguments to prove the defendant's liability." *Rodriguez v. Hayes*, 591 F.3d 1105, 1124 (9th Cir. 2010). Mr. Rodriguez, Mr. Cataldo, and Ms. Harvey use Android devices, and they will represent the Android class (Class 1); Mr. Santiago uses an Apple iOS device, and he will represent the non-Android class (Class 2). *See* Rodriguez, Cataldo, Harvey, Santiago Decls.

For many of the same reasons, Plaintiffs and their counsel will adequately represent the proposed classes. *Woods v. Vector Mktg. Corp.*, 2015 WL 5188682, at *12 (N.D. Cal. Sept. 4,

2015) ("the typicality and adequacy inquiries tend to significantly overlap."). There is no "conflict[] of interest with other class members." *Staton v. Boeing Co.*, 327 F.3d 938, 957 (9th Cir. 2003). As Plaintiffs state in their declarations, and as proven by their commitment to this case to date, Plaintiffs will "prosecute the action vigorously on behalf of the class." *Id.* The same is true of counsel, who have substantial experience with data-privacy class actions and have dedicated more than three years and substantial resources to this litigation. *See* Bonn, Lee, Yanchunis Decls.

C. Common Issues Predominate Under Rule 23(b)(3).

Predominance tests "whether the common, aggregation enabling issues in the case are more prevalent or more important than the non-common, aggregation-defeating individual issues." *Tyson Foods*, 577 U.S. at 453. Here, the legal and factual issues are common to the class and "capable of being established through a common body of evidence." *Olean Wholesale Grocery Coop., v. Bumble Bee Foods*, 31 F.4th 651, 666 (9th Cir. 2022) (en banc).

During discovery, Google repeatedly acknowledged that Plaintiffs' claims turn on common questions, which are subject to common proof. Google sought to (often successfully) limit discovery by characterizing this case as restricted to ***two* "*central questions": (1) "what Google represented to users" and (2) "the actual technical functioning of the accused technology."*** Ex. 17 at 3. Google took the position that the "[t]he facts in this case are not complicated, and the questions are straightforward." Dkt. 105 at 4. In Google's words, "***the bulk of the documents relevant to this case [are] public disclosures, Google policies, and non-public engineering documents***." Ex. 49 at 2. Google reiterated this stance over and over:

- <u>December 31, 2020</u>: Plaintiffs' claims "focus on the technical aspects of what Google did and didn't do, and whether users provided consent." Ex. 50 at 4.
- <u>February 12, 2021</u>: "Plaintiffs' claims each fall into the category of claims that rely on (1) how Google's products work, and (2) what Google told users about how its products work. . . . ***[Plaintiffs'] allegations implicate <u>only the two questions</u> identified above: what does Google say publicly, and what do its products do?***" Ex. 51 at 1–2.
- <u>November 15, 2021</u>: "The theory of the case is therefore narrow: ***(1) what Google told users about WAA, (2) how GA for Firebase works, and (3) the proper calculation of damages, if any***." Dkt. 171 at 1–2.

There should be no dispute that these "central questions" are answered with common evidence. "***This case is about,***" again in Google's own words, "***the reasonable expectations of a***

user when reading public disclosures about WAA"—an objective, on-off button. Ex. 50 at 4. There are no individualized issues that could predominate over these "central questions."

1. Common Issues Predominate for Plaintiffs' Invasion of Privacy and Intrusion Upon Seclusion Claims.

These claims are ordinarily addressed together. *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020). For both, courts "ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." MTD Order at 15 (quoting *In re Facebook*, 956 F.3d at 601). These two elements turn on an objective, "reasonable person" standard, and they can be proven with common evidence.

a. Reasonable Expectation of Privacy.

In Google's words, the relevant question is "what Google told users about WAA." Dkt. 171 at 1. This first element is satisfied if "a [(s)WAA-off] user would reasonably expect that [Google] would have access to" data relating to activity on non-Google apps while (s)WAA was off. *In re Facebook*, 956 F.3d at 602. "California law does not require Plaintiffs to prove [a] subjective expectation" of privacy. *Opperman*, 2016 WL 3844326 at *11. The focus is on the *defendant* and "the customs, practices, and circumstances surrounding [its] particular activities." *In re Facebook*, 956 F.3d at 602.

Class certification here is consistent with Judge Tigar's decision in *Opperman,* 2016 WL 3844326, at *1. There, the plaintiffs alleged that an app developer invaded their privacy by collecting contact data from their mobile devices, on which the developer's app was installed. *Id.* The court certified a Rule 23(b)(3) class, rejecting the developer's objection that "an individual inquiry will be required into the subjective expectations of each class member." *Id.* at *11. In this case, users' reasonable expectations of privacy are reflected by common, objective evidence, including Google's uniform representations regarding (s)WAA and users' decision to turn off this setting, which Google presented as a "*privacy control*." *E.g.*, Ex. 31 at 8 (July 1, 2021 Privacy Policy). Google gave users a button that promised privacy from Google, and these class members had that button "off"—their objective expectation of privacy could not be clearer. Of course this "element[] can be proven on a common basis." *Opperman*, 2016 WL 3844326, at *11.

Plaintiffs will use common evidence to prove that Google "set an expectation" that when its accountholders turned (s)WAA off, their activity on third-party apps "would not be collected." *In re Facebook*, 956 F.3d at 602. That expectation begins with the plain text of Google's statements regarding these settings. For example, throughout the Class Period, Google offered Android users (Class 1) the power to "[c]hoose the activities and info ***you allow Google to save***" by visiting the Activity Controls page with Google's (s)WAA settings. FAC ¶ 91; Dkt. 305 (Answer), ¶ 91; Ex. 19 at 3. Users of all operating systems (including both classes) visit the Activity Controls page to toggle the (s)WAA setting. Ex. 18.[4] According to that Activity Controls page, enabling both settings "***[s]aves your activity*** on Google sites and apps" as well as "activity from sites, apps, and devices that use Google services." Ex. 20.[5] The Activity Controls page also contains a link where the user can "learn more," and the hyperlinked WAA Help Page informs visitors that "Web & App Activity must be on" "[t]o ***let Google save***" information regarding "activity" on "[s]ites and apps that use Google services, including data that apps share with Google." Ex. 4.

To top it off, Google does not display (s)WAA-off app activity data on the "My Activity" dashboard that purports to show users the data Google collects from them. Hochman Rep. ¶¶ 252–53. These pages, alone and together, create the reasonable expectation that when either the WAA or sWAA button is turned off, Google will not save app activity data. *See* MTD Order at 13 (these materials create "an 'objectively reasonable expectation' that [sWAA-off users'] communications with third-party apps would not be 'recorded' by Google"). When an on-off switch is turned off, the expectation is that it is in fact off.

When Google's executives speak publicly, they likewise highlight users' supposed control over "what you choose to share." Ex. 52 at 4 (written congressional testimony of Sundar Pichai, CEO of Alphabet); Ex. 53 at 1 ("Google builds simple, powerful privacy and security tools that

[4] Before the Class Period, (s)WAA was turned off by default. Hochman Rep. ¶ 57. Through Google's "consent bump" initiative, Google tried to persuade users to give Google permission to collect app activity data by turning (s)WAA on. Schneier Rep. ¶¶ 374–382.

[5] Google's Privacy Policy defines "Google services" to include "[p]roducts that are integrated into third-party apps and sites, like ads [and] analytics." Exs. 22–35 (Privacy Policies beginning May 2018); *see* Ex. 36 at 8, Exs. 37–41 (earlier versions, similar).

keep your information safe and ***put you in control of it***.” (emphasis added)). Sundar Pichai, then Google’s CEO, testified to Congress that Google allows users to “clearly see what information we have—we actually show it back to them,” and that Google “give[s] clear toggles, by category, where [users] can decide whether that information is collected [and] stored.” Hochman Rep. ¶ 256. This is no accident: Google’s internal studies found that the prominent use of buzzwords like “control” and “choice” goes a long way toward “reassur[ing]” and “build[ing] trust” with users. Ex. 1. The more users trust Google and the controls it purports to offer, the more they use Google products—and the more money Google makes. Ex. 2 at -102 (“Increased trust and delight lead to increased loyalty, positive word-of-mouth, repurchase and other positive business outcomes.”).

While not necessary to establish a reasonable expectation of privacy, Plaintiffs’ privacy expert Bruce Schneier evaluated Google’s (s)WAA disclosures and concluded that they exemplify “dark patterns,” or “user-design tricks intended to manipulate users into doing things they wouldn’t normally choose to do.” Schneier Rep. ¶ 161. California has by statute banned the use of such dark patterns. *See* Cal. Civ. Code § 1798.140(h), (l); Cal. Code Regs. tit. 11, § 7004(b), (c).

Other documents produced by Google also provide common evidence that can resolve this issue. For example, one document demonstrates that Google has long known that “WAA just isn’t clear to users.” Ex. 54 at -39. Arne de Booij, a senior user research manager whose job was to study user expectations, predicted that ***most study participants “will believe that turning off WAA will result in no data being collected from their activity***.” Ex. 55 at -99.R. And in April 2020—a few months before this case was filed—an internal Google study found that “***all participants expected turning WAA toggle off to stop saving their activity***.” Ex. 42 at -00, -11. Even Google’s own employees thought turning WAA off stopped Google’s data collection. Google engineer Chris Ruemmler, for example, asked, “if WAA is off, how are we able to log at all?” Ex. 69. After Mr. Ruemmler learned that Google saves the data regardless of the (s)WAA settings, he wrote that Google was giving users “***a false sense of security that their data is not being stored at Google, when in fact it is***.” Ex. 7 at -09, -10 (emphasis added).

b. Offensiveness of Google's Conduct.

The second element—whether Google's conduct is highly offensive—is also subject to common proof. The standard is "highly offensive to a reasonable person," with a "focus[] on the degree to which the intrusion is unacceptable as a matter of public policy." *In re Facebook*, 956 F.3d at 606. The central factors for this analysis are common to the class: the nature of the intrusion, the "intruder's motives and objectives," the intruder's knowledge that its practices are "a problematic privacy issue," and finally broader "social norms." *Id.*

The "nature of [Google's] intrusion" is uniform classwide. *Id.* For all class members and throughout the Class Period, Google has used its Firebase and GMA SDKs to collect the same app activity data regardless of (s)WAA status. Even when (s)WAA is off, Google saves users' app activity data alongside unique, stable identifiers, and Google exploits that data for its own enrichment. Hochman Rep. §§ VII.A–B.

As technical expert Jonathan Hochman will explain, even when (s)WAA is off, Google collects detailed app activity data reflecting the apps that the user installs and visits, the amount of time spent on those apps, the pages and articles the user visits, content the user selects, videos the user watches, purchases the user makes, forms the user completed, and much more. *Id.* ¶¶ 89–91, 94–98, 122, 129. Google then saves this data alongside a host of stable identifiers (including many created and managed by Google) that pinpoint a single, unique mobile device. Hochman Rep. ¶¶ 102–111, 216–228. This data also includes the user's IP address, geolocation, device model and operating system, demographic information like age and gender, and so on. Hochman Rep. ¶¶ 89, 93, 99, 223. Google thus stockpiles information that amounts to each user's digital fingerprint, which can be used to identify individual users. *See* Hochman Rep. ¶ 304. With even a small subset of this data, locating any person's app activity data is a trivial matter. Hochman Rep. ¶¶ 328–335; Hochman Appx. B.1-D, H.1-K. As one engineer lamented, "I'm not any safer with [(s)WAA] off than on. Google will still give up any information (such as my location) for any legal investigation against me because it has the data available." Ex. 7 at -09–10.

Google also saves this data in many, many locations—so many, Google says, that it "is not practical" to identify them all, even for *Google*. Hochman Rep. ¶¶ 141, 171–77, 203–08, 230–33;

Ex. 43 at 4. Google then uses the data it collects from (s)WAA-off users to enrich itself, including by serving advertisements, measuring how these users are influenced by the ads Google shows them (and charging advertisers based on the results), measuring results of experiments run on users, training Google's machine-learning algorithms, and generally improving Google's products. Hochman Rep. § VII.F; *see also* Lasinski Rep. § 7 (calculating Google's enrichment). Google's course of conduct is uniform across the class. Hochman Rep. ¶¶ 81, 136, 268, 343.

Common evidence will also demonstrate that despite Google's uniform promises that users are in control of what it collects, Google makes it impossible for any class member to avoid Google's data vacuum. Hochman Rep. ¶¶ 249–251. Even Eric Miraglia, the founder of Google's Privacy and Data Protection Office, testified that he was "not aware of any setting" that would stop Google from collecting a user's activity on third-party apps. Ex. 4 at 96:21–97:6, 128:21–129:3. There is none. Hochman Rep. ¶¶ 249–251. And there is no point in even trying to avoid the Firebase and GMA SDKs. The GMA SDK alone is integrated with at least 80% of Android and iOS apps, and Google Analytics for Firebase is included in more than 60% of the top apps. Hochman Rep. ¶ 2. Nationwide "social norms" weigh strongly against blessing widespread and inescapable collection of sensitive data—especially from individuals who explicitly asked not to be tracked. *In re Facebook*, 956 F.3d at 606.

Common evidence will also prove that Google could have honored the (s)WAA switch to ensure that off means off. That is exactly how Google designed its App Indexing service, which is a different Firebase product primarily used to make content from non-Google apps discoverable in the Google Search app. Ex. 11 at 211:21–212:12. App Indexing also collects user data, but it reads the user's sWAA settings on the device and ***does not send data to Google if that setting is off***. Ex. 11 at 212:16–18; Ex. 56 at 113:10–11. As Google's 30(b)(6) witness explained, Google does not collect sWAA-off App Indexing data because it "doesn't add any value." Ex. 11 at 217:7–15. Google could have done the same thing with respect to Google Analytics for Firebase and the GMA SDK, Google just chose not to. Hochman Rep. ¶¶ 409–18. Why? Unlike with App Indexing, (s)WAA-off data collected by "different services like Google Analytics" or the GMA SDK *do* create revenue for Google. Ex. 11 at 217:7–15. For example, Google uses this data to track and charge its advertisers, including for valuable events driven by Google Ads, a process known as "conversion tracking" or "attribution." *See, e.g.*, Ex. 12; Ex. 13 at 218:17–219:14.

Google's knowledge and motives are similarly uniform classwide. *In re Facebook*, 956 F.3d at 606. Common evidence will prove that Google knew its promises were problematic. One Google employee, Henry Wong, wrote that "users who have turned off WAA … have given us a ***clear signal that they do not want Google to know what they are searching for*** " and "told us not to" track them. Ex. 57. Another Google employee, Chris Ruemmler, explained that "[t]he problem" is that "the wording here is ***very deceptive***," and he "fear[ed] it most likely is not" "being properly interpreted by [Google's] users." Ex. 7 at -09. "Even he "didn't realize Google actually stored all of my activity even if those controls were off and I work at Google!" *Id.* "***This is really bad***." *Id.* For years, Mr. Ruemmler pleaded to change Google's WAA disclosures to "indicate even with the control off, Google retains this data and uses it." *Id.* at -10. His concerns fell on deaf ears. Ex. 11 at 235:25–236:4. Instead, Google's WAA disclosures remained ***"intentionally vague"*** regarding Google's storage of "data that wasn't visible" to users, because "it could sound alarming." Ex. 58 at -02. As explained by Sam Heft-Luthy, then a product manager on Google's privacy team, Google's "higher-level goal" with respect to privacy is not privacy itself, but simply "giving users a *sense* of the system working to their benefit." Ex. 59 at -62. Common evidence will demonstrate that Google knew its collection and use of app activity data from (s)WAA-off users was wrong, and that Google profited handsomely from collecting and using this data anyway.

2. Common Issues Predominate for the CDAFA Claim.

Common issues also predominate for Plaintiffs' CDAFA claim. The CDAFA makes it a "public offense" to "[k]knowingly access[] and without permission take[], cop[y], or make[] use of any data from a computer, computer system, or computer network." Cal. Penal Code § 502(c)(2). "While taking or use that occurs subsequent to unauthorized access doubtless fits this description, the same goes for authorized access which turns 'unlawful [when] . . . the person without permission takes, copies, or makes use of [the] data' in question." MTD Order at 14 (citing *United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015)). Even if users might sometimes give Google permission to collect and use their app activity, those Google practices become unlawful when (s)WAA is off. *See* MTD Order at 1 (Court Order summarizing Plaintiffs' theory of liability as concerning a "Google technology that, when functioning as advertised in a given app, contravenes the company's user-facing privacy representations," i.e., the WAA disclosures).

Plaintiffs will prove their CDAFA claim with common evidence, including expert testimony from both sides grounded in Google's technical documentation. Plaintiffs' technical expert Jonathan Hochman will testify about how Google uniformly uses the Firebase and GMA SDKs to collect and save users' app activity data when (s)WAA is turned off. Hochman ¶ 85. Even Google's technical expert agrees with Mr. Hochman: "The types of app activity data sent to Google by apps that use GA4F and the GMA SDK are the same regardless of the user's account-level sWAA setting." Ex. 60 at ¶ 68. After accessing users' devices and "tak[ing]" users' app activity data "without permission," Google further violates the CDAFA by impermissibly "mak[ing] use of" the app activity data, Cal. Penal Code § 502(c)(2), including to benefit Google by measuring and attributing advertising conversions. Hochman § VII.F.

Google lacks permission to take and use the app activity data because, through its uniform disclosures, Google represented setting (s)WAA to "off" would prevent Google from collecting and saving users' app activity. In fact, Google not only failed to obtain permission to take and use the app activity data, but Google also had an explicit notification that it lacked such permission by virtue of the affirmative choice to set (s)WAA to "off." As succinctly summarized by yet another concerned Google employee, Elyse Bellamy, "we don't (as a company) have a very even approach to determining what we need to ask permission for." Ex. 61 at -84. Addressing WAA, another employee stated that "much of the language intended to be comprehensive feels vague and hard-to-parse for non-engineers/lawyers." Ex. 62 at -80. Other employees recognized that WAA "is just fundamentally difficult to get." Ex. 68 at -97. And as explained by Google engineer Chris Ruemmler during his deposition in this case:

> [B]ack before I had more knowledge about the way WAA works...I thought at that time if the opposite of on and off, if it was off, well, we just didn't, you know, send any of this data to Google. But that's not right.

Ex. 63 at 72:21–73:3. The truth is distinctly Orwellian. At Google, "off" is not the opposite of "on," and what you "allow Google to save" is irrelevant because Google will save it anyway.

Harris v. comScore, Inc. is instructive. 292 F.R.D. 579 (N.D. Ill. 2013). Like here, the plaintiffs alleged that the defendant improperly obtained and used their online activity, in violation of the Computer Fraud and Abuse Act ("CFAA"), which is the federal analog for the CDAFA. *Id.* at 581. The court certified that claim under Rule 23(b)(3), reasoning that "plaintiffs raise a variety of common questions that can be resolved on a classwide basis" because "the software attempts to collect the same information from all computers, and the question of whether that collection exceeds the scope of consent is common to all plaintiffs." *Harris*, 292 F.R.D. at 585. The same outcome is warranted here because whether Google's data collection and use exceed the scope of permission likewise turns on the defendant's uniform disclosures to users.

Plaintiffs will also rely on common evidence to meet the CDAFA's "damage or loss" requirement. Cal. Penal Code § 502(e)(1). Plaintiffs' damages expert Michael Lasinski will testify that Google earned at least hundreds of millions of dollars from its collection, saving, and use (s)WAA-off app activity data. Lasinski Rep. ¶¶ 79, 114. Such unjust enrichment constitutes "damage or loss" sufficient to support a claim under the CDAFA. *See In re Facebook*, 956 F.3d at 600 (sustaining CDAFA claim where plaintiffs alleged that Facebook was unjustly enriched by collecting their browsing data, holding that "California law recognizes a right to disgorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss."). Mr. Lasinski also demonstrates that there is a market for this type of data, and Plaintiffs were deprived of the opportunity to sell their data to Google within this market. Lasinski Rep. § 8.

Google's collection of app activity data also caused harm by draining Plaintiffs' devices of their battery-life and causing them to run more slowly. *See, e.g.*, Ex. 13 at 138:19–23; Schneier Rep. ¶ 102 (advertising on a mobile device "is an enormous drain on computing resources"); Ex. 64 at -10 (Google document explaining the effect of Google Analytics on devices' "battery life"); Ex. 65 at -98 (Google document admitting that "pok[ing]" the "connection to a server from a device" can "consume a lot of battery"). Such harm independently constitutes "damage or loss" under the CDAFA. *In re Carrier IQ, Inc., Consumer Privacy Litig.*, 78 F. Supp. 3d 1051, 1066–67 (N.D. Cal. 2015).

3. Users' Expectations Cannot Defeat Predominance.

As explained above, Rule 23(b)(3) certification is appropriate because "one or more of the central issues in the action are common to the class and can be said to predominate," including the two central questions Google repeatedly identified. *Tyson*, 577 U.S. at 453. Google may now seek to abandon its position and conjure up purportedly individualized issues, such as users' subjective expectations. As a threshold matter, certification is "proper under Rule 23(b)(3) even [if] other important matters will have to be tried separately." *Id.* But here, no central issue turns on individualized inquiries. Users' expectations about these objective buttons are no exception.

The claims here turn on an objective, reasonable user standard. *See Opperman,* 2016 WL 3844326, at *11 (certifying Rule 23(b)(3) class for invasion of privacy and rejecting argument that individual inquiries are required). Privacy claims "can be proven on a common basis." *Id.* The same is true for the CDAFA, which focuses on whether the defendant had "permission" to collect and use the data. Cal. Penal Code § 502(c)(2). Permission requires something conveyed from one person to another. It is defined "as the 'act of permitting' or 'a license or liberty to do something; authorization.'" *Carrier IQ*, 78 F. Supp. 3d at 1100 (discussing CDAFA's "without permission" requirement). Absent any exchange between Google and the user, someone's individual expectations do not give rise to an "act" or "license" for Google to collect and use data.

Regardless, individualized inquiries are unnecessary. This case is about an *on-off toggle* that Google offers to all class members, which was turned off for every class member. The meaning of this signal is self-evident. As summarized by Google employee Chris Ruemmler, "a light is on, a light is off; right? You know, that's the opposite behavior. And so I think ***I had a misconception that when WAA was off, there was no logging performed***." Ex. 63 at 135:20–136:1. There is no need for individual inquiries. Off just means off.

Google may attempt to misdirect the Court, pointing to third-party apps' privacy policies that mention their use of Google Analytics. The argument Google advances—that the mere mention of Google Analytics overrides the user's explicit and specific rejection of consent through the (s)WAA button—is nonsense. The (s)WAA setting covers activity on apps that use Google services; if an app's general disclosure of those services amounts to consent, then the (s)WAA setting is meaningless. And indeed, Google has never identified a *single* app privacy policy disclosing that Google collects data from *all* users, regardless of (s)WAA setting (or any other privacy setting). Whatever a user's agreement with third-party apps, (s)WAA-off users are assured that *Google* will not collect, save, or use app activity data.

4. Common Issues Predominate for the Monetary Relief Sought.

Plaintiffs will also rely on common evidence to establish the monetary relief to which the classes and their constituents are entitled. Plaintiffs seek four forms of monetary relief: disgorgement, actual damages, punitive damages, and nominal damages. Each is "'capable of measurement on a classwide basis,' in the sense that the whole class suffered damages traceable to the same injurious course of conduct." *Just Film, Inc. v. Buono*, 847 F.3d 1108, 1120 (9th Cir. 2017) (quoting *Comcast Corp. v. Behrend*, 569 U.S. 27, 34–35 (2013)).[6] Much of this evidence is provided by an expert, Michael Lasinski, who adapted methodologies that Google uses in the ordinary course of business to the at-issue conduct—methodologies another Court in this District determined to reliably estimate unjust enrichment and damages. *Brown v. Google, LLC*, 2022 WL 17961497, at *3–7 (N.D. Cal. Dec. 12, 2022) (denying motion to exclude Lasinski's damages models in a case about Google's collection and use of data).

a. Disgorgement.

The amount by which Google was unjustly enriched—and the profits Google must disgorge—is a common issue, and it will be proven with common evidence. *In re Facebook*, 956 F.3d at 600 (recognizing "right to disgorgement of profits"). Google often analyzes the impact that contemplated privacy and advertising settings will have on its bottom line. Lasinski Rep. § 6.7. Using Google's own methodologies from internal studies of the revenue impact from settings that affect the same types of revenue-generating activities at issue in this case (i.e., serving ads and tracking conversions), Mr. Lasinski conservatively estimated Google's profits through 2022 from *just two* of many ways it used the wrongfully collected data: By using (s)WAA-off data to track

[6] Even if damages could not be determined with common evidence, the Ninth Circuit has repeatedly affirmed that "damage calculations alone cannot defeat class certification." *Pulaski & Middleman, LLC v. Google, Inc.*, 802 F.3d 979, 986 (9th Cir. 2015); *Olean*, 31 F.4th at 668–69 (collecting cases).

conversions, Google earned about $558 million in net revenues; that figure increases to $665 million by including Google's use of (s)WAA-off data to serve advertisements. Lasinski Rep. § 1.

To determine profits attributable to conversion-tracking, Mr. Lasinski employed the same methodology Google used when it quantified the revenue it stood to lose when another setting inhibited Google's ability to track conversions (i.e., following a user from ad to action) on the web: (1) start with the total Google revenue from the at-issue revenue streams (here, ads for apps ("App Promo"), AdMob, and app-specific Ad Manager revenues); (2) multiply by the percentage of activity subject to the relevant restriction (here, (s)WAA-off app activity); and (3) multiply again, by the percentage of ad revenue bid against the relevant conversions (here, App Promo revenue bid against Firebase conversions, and AdMob and Ad Manager revenues bid against all conversions). Lasinski Rep. § 7.1. Mr. Lasinski identified inputs from Google's own documents, then subtracted costs Google incurred because of its wrongful conduct. *See, e.g.*, Lasinski Rep. ¶¶ 83–85, 88, 89, 91, 106–07, 110–11. Mr. Lasinski ultimately concluded that from July 2016 through 2022, Google made $558 million by using the at-issue data for conversion tracking. *Id.* ¶ 112.

Mr. Lasinski also calculated Google's profits attributable to its use of (s)WAA-off data to serve ads. According to Google, (s)WAA-off ads are less valuable because Google does not use (s)WAA-off app activity data to personalize ads. Lasinski Rep. ¶¶ 44, 120. Google studied the revenue impact of ads personalization and concluded that a non-personalized ad generates about half as much revenue for Google as a personalized ad. Lasinski Rep. ¶ 120. Mr. Lasinski imported that conclusion into Google's tried-and-true methodology: Google's profits from serving (s)WAA-off ads equals (1) the total revenue streams at issue, (2) multiplied by the percentage of (s)WAA-off app activity, (3) multiplied again by the portion of ad revenue *not* attributable to personalization. Lasinski Rep. § 7.2. After subtracting Google's costs, Google through 2022 made about $664 million from serving and monetizing ads to (s)WAA-off users. Lasinski Rep. ¶ 129.

b. Distributing Disgorged Profits.

"[A]ll that plaintiffs need to prove" is that aggregate damages are "calculable," and Plaintiffs have done so. Newberg on Class Actions § 12:2. The "partitioning" of an aggregate damage award "among class members may lead to individual calculations," but "those calculations would not impact a defendant's liability for the total amount of damages," and they "do not defeat class certification." *Ruiz Torres v. Mercer Canyons*, 835 F.3d 1125, 1140–41 (9th Cir. 2016). The defendant has "no interest in the method of distributing the aggregate damages award among class members." *In re Urethane Antitrust Litig.*, 768 F.3d 1245, 1269 (10th Cir. 2014), *cited with approval in Olean*, 31 F.4th at 669. If the claims require inquiry into "[i]ndividual damages," those questions can "be worked out later or in subsequent proceedings." Newberg on Class Actions § 12:2; *see In re Urethane*, 768 F.3d at 1269 (approving post-verdict claims process for distributing aggregate, class-wide judgment of over $1 billion). "[W]ith respect to Lasinski's method of apportionment, Google does not have standing to complain." *Brown*, 2022 WL 17961497, at *7.

Notwithstanding clear Ninth Circuit law that the defendant has no stake in the distribution of an aggregate award, Plaintiffs have proposed a method to distribute damages in a post-trial claims process. As Mr. Lasinski explains, disgorged profits can be divided by the total number of "sWAA-Off User Months," where each "sWAA-Off User Month" represents a month in which an individual in the United States used a mobile device with sWAA off. Lasinski Rep. § 9.2.2. Each class member's share would be determined by the months they had (s)WAA off, as demonstrated by Google records reflecting users' sWAA status throughout the Class Period. Lasinski Rep. ¶ 174; Hochman Rep. ¶¶ 147–151. Alternatively, and especially if Google's deletion of class members' app activity data limits such allocation, damages can also be allocated per capita. Lasinski Rep. § 9.2.1; Dkt. 167 at 3–5 (describing and defending Google's refusal to preserve class members' app activity data). This is an accepted allocation method. *See Hale v. State Farm Mut. Auto. Ins. Co.*, 2016 WL 4992504, at *8 (S.D. Ill. Sept. 16, 2016). Plaintiffs' unrebutted legal notice expert also explains why notice in this case is feasible. *See generally* Azari Rep. § IV. Class members can be contacted easily, including by sending notice to the email address(es) associated with Google Accounts that had (s)WAA off at any time during the Class Period. Azari Rep. § IV.A.

c. Actual Damages.

Actual damages (including restitution) can also be calculated classwide using common evidence. Mr. Lasinski quantified the value of class members' data that Google unlawfully collected, relying on an internal Google project known as the "Ipsos Screenwise Panel." Through this program, Google pays people to let Google track their activity on a device, including mobile devices. Lasinski Report ¶¶ 135, 139. Google's payments to users can exceed $16 per month. *Id.* ¶ 142. But Mr. Lasinski selected the program's minimum payment for a single device ($3 per month) as a conservative indicator of the payment necessary for an individual to allow Google to track their app activity. *Id.* ¶ 151. Although Google pays participants $3 *per month*, Mr. Lasinski calculated actual damages in a more conservative way, applying this $3 payment on a *one-time basis*, for each mobile device used with (s)WAA off during the Class Period. *Id.* As another Court held, this figure approximates both restitution and the value associated with the peace of mind from knowing that Google is not watching. *Brown*, 2022 WL 17961497, at *5. Mr. Lasinski also used internal Google data to quantify the number of class members devices, totaling 162,015,424 across the two classes and for the full Class Period. *Id.* ¶¶ 152–59. Multiplying that input by $3 per device, Mr. Lasinski calculated that Google would have had to pay at least $486 million to persuade class members to give up their data and their peace of mind. *Id.* ¶ 161.

d. Punitive Damages.

Punitive damages are available for all three claims.[7] Because "the purpose of punitive damages is not to compensate the victim, but to punish and deter the defendant, . . . the focus of a punitive damages claim is not on facts unique to each class member, but on the defendant's conduct toward the class as a whole." *Ellis v. Costco Corp. III*, 285 F.R.D. 492, 542–44 (N.D. Cal. 2012) (certifying Rule 23(b)(3) class, including for purposes of seeking punitive damages). Plaintiffs will rely on common evidence, including internal documents establishing that Google knew its disclosures were misleading. *See supra* Section II.C.1.

D. Plaintiffs Have Article III Standing.

In the Ninth Circuit, "the standing inquiry is concluded" for purposes of class certification "once the named plaintiff demonstrates her individual standing to bring a claim." *Melendres v. Arpaio*, 784 F.3d 1254, 1262 (9th Cir. 2015). Plaintiffs have many bases for standing.

[7] *See* Cal. Penal Code § 502(e)(4) (CDAFA); *Condon v. Condon*, 2008 WL 11338437, at *7 (C.D. Cal. June 6, 2008) (privacy).

Google robbed each Plaintiff of their right to privacy, an injury "traditionally recognized as providing a basis for lawsuits in American courts." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021); *In re Facebook*, 956 F.3d at 598 (privacy violations "have long been actionable at common law" (citations omitted)). "The intrusion itself makes the defendant subject to liability"; no further injury is required. *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1117 (9th Cir. 2020). The Named Plaintiffs and the putative class members also have standing by virtue of their "stake" in Google's "profits from [their] personal data." *Facebook Tracking*, 956 F.3d at 600 (holding that this "stake," provided by California law, is "sufficient to confer Article III standing"). Moreover, Google leached battery life and bandwidth from Plaintiffs' devices to advance Google's business interests when it took their data without permission. *See* Section II.C.2. These injuries are substantiated by Plaintiffs' declarations, testimony, and expert opinions. *See* Rodriguez, Cataldo, Harvey, Santiago Decls.; Section II.C.4. At this stage, no more is required.

E. A Class Action Is a Superior Method of Adjudication.

A class action under Rule 23(b)(3) is superior because it will achieve "economies of time, effort, and expense" while promoting "uniformity of decisions as to persons similarly situated." *Amchem Products v. Windsor*, 521 U.S. 591, 615 (1997). Discovery involved a substantial amount of time, effort, and expense. Plaintiffs reviewed over 2 million pages of documents that Google produced (including from 28 Google custodians), took and defended 25 depositions, and retained five testifying experts. "[G]iven the high costs of litigation, the need for expert opinion, and the risks involved, individual suits likely would not make economic sense for a substantial number of putative class members." *Gold v. Lumber Liquidators, Inc.*, 323 F.R.D. 280, 293 (N.D. Cal. 2017) (Seeborg, J.). Here, "class treatment is likely to reduce litigation costs and promote efficiency relative to trying each case individually." *McCowen v. Trimac Transp. Servs. (W.), Inc.*, 311 F.R.D. 579, 589 (N.D. Cal. 2015) (Seeborg, J.).

"Rule 23 does not require a class proponent to proffer an administratively feasible way to identify class members." *Pettit v. Procter & Gamble Co.*, 2017 WL 3310692, at *2 n.1 (N.D. Cal. Aug. 3, 2017) (Seeborg, J.) (citing *Briseno v. ConAgra Foods, Inc.*, 844 F.3d 1121, 1133 (9th Cir. 2017)). "In this Circuit, it is enough that the class definition describes a set of common characteristics sufficient to allow a prospective plaintiff to identify himself or herself as having a right to recover based on the description" of the class. *McCrary v. Elations Co., LLC*, 2014 WL 1779243, at *8 (C.D. Cal. Jan. 13, 2014). Here, class members could readily self-identify. The classes are limited to Google accountholders who used non-Google apps including the Firebase or GMA SDKs while (s)WAA was off. Nearly everyone who used a mobile device with (s)WAA off meets the criteria. Firebase alone is so widespread that using just five random non-Google apps creates a 97% chance of having data collected by these Google SDKs. Hochman Rep. ¶¶ 355–56.

While unnecessary, Google can use its records to identify class members or verify claims. Hochman Rep. § VII.I. Google admitted it "reliably tracks WAA and sWAA on-and-off events for all Google Account Ids." Ex. 66 at 12. That means Google has a list of all WAA-off and sWAA-off users. Google also knows which apps use the at-issue SDKs. Hochman Rep. ¶¶ 350–53; *see also, e.g.*, Ex. 67 at 31–45 (verifying which of the Plaintiffs' apps use Firebase). Based on his analysis of data Google produced, Mr. Hochman concluded that Google's records of app activity (to the extent preserved) can also be used for this purpose. Hochman § VII.I; *see also supra* Section II.C.1.b (explaining why the at-issue data is identifying). "Any claims administration process can be designed to ensure Defendants are offered a mechanism to challenge individual class members' claims to ensure they are not compensated unjustifiably." *In re Xyrem Antitrust Litig.*, 2023 WL 3440399, at *4 (N.D. Cal. May 12, 2023) (Seeborg, J.); *see also* Azari Rep.

F. Rule 23(b)(2) Certification Is Also Warranted.

Plaintiffs also seek Rule 23(b)(2) certification to obtain equitable relief. "Rule 23(b)(2) does not require [courts] to examine the viability or bases of class members' claims for declaratory and injunctive relief, but only to look at whether class members seek uniform relief from a practice applicable to all of them." *Ward v. United Airlines, Inc.*, 2021 WL 534364, at *7 (N.D. Cal. Feb. 12, 2021) (quoting *Rodriguez v. Hayes*, 591 F.3d 1105, 1125 (9th Cir. 2010)). The focus "is not on the claims of individual class members, but rather whether [a defendant] has engaged in a 'common policy.'" *In re Yahoo Mail Litig.*, 308 F.R.D. 577, 599–600 (N.D. Cal. 2015); *Burdick v. Union Sec. Ins. Co.*, 2009 WL 6541608, at *16 (C.D. Cal. April 2, 2009) (same).

Here, Plaintiffs (on behalf of the two classes) seek uniform relief from Google's ongoing collection, storage, and use of (s)WAA-off app activity data. Plaintiffs specifically seek an order: (1) precluding Google from further collecting, storing, and using consumers' (s)WAA-off app activity data; (2) requiring Google to delete already collected (s)WAA-off app activity data; (3) requiring Google to delete any products, services, or algorithms built in whole or in part with that unlawfully collected (s)WAA-off app activity data; and (4) appointing an independent third party to verify that the injunctive relief has been (and continues to be) implemented. Plaintiffs' requested relief is sufficiently detailed at this juncture. Rule 23(b)(2) "ordinarily will be satisfied when plaintiffs have described the general contours of an injunction that would provide relief to the whole class, that is more specific than a bare injunction to follow the law, and that can be given greater substance and specificity at an appropriate stage in the litigation." *Parsons v. Ryan*, 754 F.3d 657, 689 n.35 (9th Cir. 2014).

Injunctive relief here would bring "important changes to reflect transparency in the system." *Brown*, 2022 WL 17961497, at *20 (certifying classes under Rule 23(b)(2) for seven claims—including invasion of privacy, intrusion upon seclusion, and the CDAFA—where the plaintiffs seek similar equitable relief related to Google's collection, storage, and use of data). Courts routinely certify cases under Rule 23(b)(2) pursuing such relief. *See, e.g.*, *DZ Rsrv. v. Meta Platforms, Inc.*, 2022 WL 912890, at *1, 9 (N.D. Cal. Mar. 29, 2022) (certifying injunctive relief class seeking to require Meta to correct/cease certain advertising practices); *Yahoo Mail Litig.*, 308 F.R.D. at 600 (certifying injunctive class demanding that Yahoo to stop scanning emails and "permanently delete all data it has collected and stored . . . without consent"). Finally, this Court may certify the claims under both Rule 23(b)(3) and Rule 23(b)(2). *In re Xyrem*, 2023 WL 3440399, at *12 (certifying claims under both Rule 23(b)(3) and (b)(2)).

III. CONCLUSION

Plaintiffs respectfully request that the Court certify both classes under Rule 23(b)(3) and Rule 23(b)(2), appoint Plaintiffs as class representatives, and proposed counsel as class counsel.

Dated: July 20, 2023 Respectfully submitted,

By: /s/ Mark Mao

Mark C. Mao (CA Bar No. 236165)
mmao@bsfllp.com
Beko Reblitz-Richardson (CA Bar No. 238027)
brichardson@bsfllp.com
BOIES SCHILLER FLEXNER LLP
44 Montgomery Street, 41st Floor
San Francisco, CA 94104
Telephone: (415) 293 6858
Facsimile (415) 999 9695

David Boies (admitted *pro hac vice*)
dboies@bsfllp.com
BOIES SCHILLER FLEXNER LLP
333 Main Street
Armonk, NY 10504
Telephone: (914) 749-8200

James Lee (admitted *pro hac vice*)
jlee@bsfllp.com
Rossana Baeza (admitted *pro hac vice*)
rbaeza@bsfllp.com
BOIES SCHILLER FLEXNER LLP
100 SE 2nd Street, Suite 2800
Miami, FL 33131
Telephone: (305) 539-8400
Facsimile: (305) 539-1307

Alison L. Anderson, CA Bar No. 275334
alanderson@bsfllp.com
M. Logan Wright
mwright@bsfllp.com
BOIES SCHILLER FLEXNER LLP
725 S. Figueroa Street, 31st Floor
Los Angeles, CA 90017
Telephone: (813) 482-4814

Bill Carmody (*pro hac vice*)
bcarmody@susmangodfrey.com
Shawn J. Rabin (*pro hac vice*)
srabin@susmangodfrey.com
Steven Shepard (*pro hac vice*)
sshepard@susmangodfrey.com
Alexander P. Frawley
afrawley@susmangodfrey.com
Ryan Sila
rsila@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019

Telephone: (212) 336-8330

Amanda Bonn (CA Bar No. 270891)
abonn@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Telephone: (310) 789-3100

John A. Yanchunis (*pro hac vice*)
jyanchunis@forthepeople.com
Ryan J. McGee (*pro hac vice*)
rmcgee@forthepeople.com
Michael F. Ram (CA Bar No. 238027)
mram@forthepeople.com
MORGAN & MORGAN, P.A.
201 N Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 222-4736

Attorneys for Plaintiffs